PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 010055B1WO	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US02/16103	International filing date *(day/month/year)* 21 May 2002 (21.05.2002)	Priority date *(day/month/year)* 22 May 2001 (22.05.2001)
International Patent Classification (IPC) or national classification and IPC IPC(7): H04L 9/00 and US Cl.: 380/264		
Applicant QUALCOMM INCORPORATED		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

□ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 0 sheets.

3. This report contains indications relating to the following items:

I ☒ Basis of the report

II □ Priority

III □ Non-establishment of report with regard to novelty, inventive step and industrial applicability

IV □ Lack of unity of invention

V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

VI □ Certain documents cited

VII □ Certain defects in the international application

VIII □ Certain observations on the international application

Date of submission of the demand 19 December 2002 (19.12.2002)	Date of completion of this report 19 March 2003 (19.03.2003)
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer for Aravind K Moorthy James R. Matthews Telephone No. 703-305-1373

INTERNATIONAL PRELIMINARY EXAMINATION REPORT	International application No. PCT/US02/16103

I. Basis of the report

1. With regard to the elements of the international application:*

☒ the international application as originally filed.

☒ the description:
pages 1-18 as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of ______________.

☒ the claims:
pages 19-22, as originally filed
pages NONE, as amended (together with any statement) under Article 19
pages NONE, filed with the demand
pages NONE, filed with the letter of ______________.

☒ the drawings:
pages 1-5, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of ______________.

□ the sequence listing part of the description:
pages NONE, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of ______________.

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

□ the language of a translation furnished for the purposes of international search (under Rule23.1(b)).

□ the language of publication of the international application (under Rule 48.3(b)).

□ the language of the translation furnished for the purposes of international preliminary examination(under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

□ contained in the international application in printed form.

□ filed together with the international application in computer readable form.

□ furnished subsequently to this Authority in written form.

□ furnished subsequently to this Authority in computer readable form.

□ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

□ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☒ the description, pages NONE
☒ the claims, Nos. NONE
☒ the drawings, sheets/fig NONE

5. □ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*
** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US02/16103

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims	1-17	YES
	Claims	NONE	NO
Inventive Step (IS)	Claims	1-17	YES
	Claims	NONE	NO
Industrial Applicability (IA)	Claims	1-17	YES
	Claims	NONE	NO

2. CITATIONS AND EXPLANATIONS
Please See Continuation Sheet

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

V. 2. Citations and Explanations:

Claims 1-17 meet the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest what is disclosed in the claims.

As to claims 1-7, "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest generating a plurality of keys in response to a received challenge. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest generating an initial value based upon a first key from the plurality of keys. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest concatenating the initial value with a received signal to form an input value, where the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest that the second key has been communicated from the subscriber identification module to the communications unit. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest hashing the input value to form an authentication signal and transmitting the authentication signal to the communications system via the communication unit.

As to claim 8-10, "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest a key generation element. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest a signature generator configured to receive a secret key from the key generation element and information from a mobile unit and further configured to generate a signature that will be sent to the mobile unit. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest that concatenating the secret key with the information from the mobile unit and hashing the concatenated secret key and information generate the signature.

As to claims 11-14, "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest a key generator for generating a plurality of keys from a received value and a secret value. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest that at least one communication key from the plurality of keys is delivered to the communications unit. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest that at least one secret key from the plurality of keys is not delivered to the communications unit. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest a signature generator for generating an authorization signal form hashing a version of at least one secret key together with an authorization message. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest that the communications unit using a version of at least on communication key generates the authorization message.

As to claims 15-17, "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest generating a plurality of keys. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest generating a signature at the communications device using both the key transmitted to the communications device and a transmission message. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest that the generating is implemented by hashing a concatenated value formed from at least one key and the transmission message. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest transmitting the signature to the subscriber identification device or receiving the signature at the subscriber identification device. "Rogues MS-Shell Threat Analysis" does not teach or fairly suggest generating a primary signature from the received signature, where the generating is implemented by hashing a concatenated value formed from the one private key and the signature received from the communications device. "Rogues

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US02/16103

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

MS-Shell Threat Analysis" does not teach or fairly suggest conveying the primary signature to a communications system.

Claims 1-17 meet the criteria set out in PCT Article 33(4), and thus meet industrial applicability because method and apparatus for providing local authentication of subscribers traveling outside their home systems can be made or used in industry.

---------------- NEW CITATIONS ----------------